

Det nytter ikke at stikke hovedet i sandet!

De fleste IT afdelinger bruger logs efter **strudsemetoden**, men det nytter ikke at "**stikke hovedet i sandet**", når det gælder IT-sikkerhed.



Strudsemetoden!

■ Vi definerer **strudsemetoden** som den "brug" af logs, hvor man sent i et forløb opdager et problem og derefter manuelt går tilbage på en server / switch og søger igennem loggen for at se, om man kan finde et problem.

Eller lader sine switches (og måske også servere) sende alle syslogs ind i en fælles base og så glemmer alt om dem. Denne fælles "**skraldespand**" gør det meget besværligt efterfølgende at søge i logs og der er ingen proaktiv korrelering.

Med andre ord: Man bruger **ikke** logs aktivt.

Gør mere end blot at indsamle logs!

Deltag i vores **Log Management** webinar fredag den 25. februar 2011 kl. 10.00-11.00

- Tilmeld dig på vores hjemmeside www.draware.dk/events/ senest den 22. februar 2011 kl. 18.00 og se en produktspecifik løsning fra ImmuneSecurity.
- Du kan læse mere om Log Management og LogInspect fra ImmuneSecurity på vores hjemmeside www.draware.dk/emne/log-management/, du også meget velkommen til at skrive os en e-mail på info@draware.dk eller ringe til en af vores Log Management eksperter på tel: (+45) 45 76 20 21.

God læselyst og venlig hilsen

Draware™ A/S

A handwritten signature in blue ink, appearing to read 'Christian Schmidt'.

Christian Schmidt, Direktør (chr@draware.dk)

Benytter du strudsemetoden?

■ Det betyder **ingen** indsamling, **ingen** proaktiv anvendelse og kun en reaktiv brug af logs ved at dykke ned i device log for at finde **nålen i høstakken**, som måske kan give et fingerpeg om en driftsforstyrrelse eller en sikkerhedsbrist.

■ Hvorfor ikke bruge dine logs **proaktivt**, så du udover at kunne søge i alle dine logs et samlet sted også får **automatisk** besked når dine logs fortæller dig noget du SKAL være **opmærksom** på?

Følg os på:



www.youtube.com/draware